Counting

James Philip Rowell

There are 10 sorts of people in the world: those who understand binary and those who don't.

What does "10" mean?

We got it drilled into us watching Sesame Street that "10" is the symbol for the number "ten" which is this many apples "🍎🍎🍎🍎🍎🍎🍎🍎🍎🍎" or the number of fingers on a typical person's two hands.

Once we are trained to automatically think of "10" as representing ten things, we quickly move past it to learn about 100 and 1000 and how to interpret a string of digits like 92507. Even at a young age we'd be able to accurately count out a pile of ninety-two-thousand-five-hundred-and-seven apples as time-consuming and agonizing as it might be. Furthermore, learning how to add and multiply is easy once you can count in base-ten since the techniques are simple and straight-forward.

What about kids in ancient Rome, was it as easy for them? Try adding two numbers together in ancient Rome, or worse, multiplying or dividing them. What's XI times IX? Would you believe me if I told you it's XCIX?

Unless you convert those to Hindu-Arabic decimal or base-ten numbers to check, you're just gonna have to trust me. Truth is - I don't know how to multiply using Roman numerals - nor did most Romans. Not only that, but I'll bet that most modern eight-year-olds can count higher than any Roman could - as the Roman system only effectively allowed counting up to 4999.

Even though the ancient Romans and us use different symbols, we are talking about the same abstract set of numbers underneath which we call integers[*]. Mathematics deals with numbers in this pure sort of way, divorced from the symbols used to represent each number. When we talk about positive integers in mathematics, it's best to remind yourself that we're really talking about different sized piles of apples. Each successive number represents the quantity of successively larger piles of apples - i.e.; try to forget about the specific symbols we use like "9" and "10" or "IX" and "X" and think about each integer as a specific sized pile of apples.

However, we use numbers written out in base-ten all the time in mathematics, rarely thinking in terms of piles of apples. We take for granted that we can use base-ten to represent the set of positive integers, but, we should be careful about what we take for granted as the only ideas that modern-mathematics takes for granted are axioms. The fact that we can use base-ten to represent the integers is NOT among the list of axioms.

Briefly; the axioms describe a few simple properties about addition and multiplication. These properties are *so simple* that they can't be expressed in yet other even-simpler ideas. The

[*] Integers are the set of all the positive whole numbers, as well as zero and all the negative counterparts to each positive number.

axioms are the minimal set of simple, obvious, irrefutable ideas from which everything else in mathematics is built*.

Since our ability to count in base-ten is not axiomatic, then to properly ground it in modern-mathematics we should define what it means to write out a number in decimal, state its properties in a theorem, then provide a proof of that theorem - The proof being a series of arguments that logically connects it directly† to the axioms. In doing so, the only way that the theorem could be false is if the axioms themselves are false.

Here's what that theorem looks like.

Basis Representation Theorem

> Let b be a positive integer greater than 1.
>
> For every positive integer n there is a unique sequence of integers $d_0, d_1, d_2, \dots, d_k$ such that:
>
> $$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0,$$
>
> where $0 \leq d_i < b$ for all i in $\{0, 1, 2, \dots, k\}$ and $d_k \neq 0$.
>
> Definition: n is represented in base-b by the string of base-b-digits $(d_k d_{k-1} \cdots d_2 d_1 d_0)_b$

"That's nuts!" you might say, I don't even see a "ten" in there so how could that describe how we learned to count watching Sesame Street? If you're unfamiliar with mathematical notation then that stuff above likely probably looks like nonsense.

Try this: imagine that the above was written such that we replace the b with "ten". Does it make any more sense? At least then we'd have the "Base-Ten Representation Theorem". We could also let $b = 2$, which would give us the "Base-Two Representation Theorem" stating how we count in binary.

Anyway, don't worry if you can't read the theorem, we'll get to how to do that shortly, but this theorem is a good example of the kind of thing mathematicians like to do - generalize ideas.

Why restrict ourselves to ten when the idea applies equally well to two, three, four, five, ... etc.? The heptapods in "Arrival" have seven limbs with seven fingers each, perhaps they use base-forty-nine, so our theorem should cover that case too. By generalizing the idea to a base b, where b is any number two or higher (base-one doesn't really make sense - think about it for a while‡), we gain a deeper understanding of the subject in question.

Even though doing arithmetic in base-ten has been going on for almost two-thousand years, formalizing it and generalizing it into a theorem is fairly modern. The earliest reference I've found to our theorem is in "Elementary Number Theory" by E. Landau in 1958. We probably don't need to look further back than Leibniz time when he introduced the idea of binary arithmetic in 1679. So our theorem is fairly recent on the world stage.

---

*The axioms: For every integer a, b and c: Associativity: $(a + b) + c = a + (b + c)$ and $a(bc) = (ab)c$; Commutativity: $a + b = b + a$ and $ab = ba$; Distributive: $a(b + c) = (b + c)a = ab + ac$; Identities: There are integers 0 and 1 ($0 \neq 1$) such that, $a + 0 = 0 + a = a$ and $a \cdot 1 = 1 \cdot a = a$ and Additive Inverse: $a + (-a) = 0$. Note: in general integers do NOT have multiplicative inverses that are also integers. (eg. $\frac{1}{2}$ is the multiplicative inverse of 2 because $\frac{1}{2} \cdot 2 = 1$ but $\frac{1}{2}$ is not an integer.)

†directly ... or indirectly via other previously proven theorems.

‡Is base-one essentially a pile of apples?

Assuming you want to be able to make sense of and read our theorem, then let's take a step back and work up to its statement, using our familiar base-ten for discussion.

When using an arbitrary base (i.e.; base-b) to count with, it's useful to have simple symbols to represent each of the integers from zero to up to $(b-1)$. So in our base-ten system we use the digits 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9.

Base-ten strings a series of these digits together one after the other to be able to represent each positive integer. Let's look at the first two-digit-number, that is, ten, which as you well know looks like this: "10". This extra digit on the left tells us how many tens we have and the last, or rightmost digit says how many additional units to add to it.

So our very first two-digit-number 10 means "one lot of ten - plus zero units". When we see "11" - we interpret it to mean "one lot of ten - plus one unit", and "12" is "one lot of ten - plus two units", etc.

Continuing on; "20" - we interpret to mean "two lots of ten, plus zero units", etc. up to "90" meaning "nine lots of ten, plus zero units".

Following this line of reasoning since "10" now means the integer ten, then "100" must mean "ten lots of ten, plus zero units"- which is exactly what it means. We have a special word for this number we call it "one-hundred" or "one lot of a hundred, plus zero lots of tens, plus zero units". Similarly "200" means "two lots of a hundred, plus zero lots of ten, plus zero units", etc.

We can keep going by one-hundred until we similarly get to "1000" or "ten lots of a hundred, plus zero lots of ten, plus zero units" otherwise known as "a thousand" or "one lot of a thousand, plus zero ...etc".

It gets a little tedious to be so specific when reading out a number so our language has developed quite a few verbal shortcuts. Furthermore, it doesn't take long before we run out of fancy names for these "powers-of-ten" like, million, billion, trillion, zillion etc. So let's introduce some nice clean mathematical notation to describe these powers-of-ten and let's forget the fancy words.

$$\begin{aligned}
100 &= 10 \times 10 = 10^2, \\
1000 &= 10 \times 10 \times 10 = 10^3, \\
10000 &= 10 \times 10 \times 10 \times 10 = 10^4, \\
&\dots \\
\underbrace{10\dots000}_{\text{k zeros}} &= \underbrace{10 \times 10 \times 10 \times 10 \times \dots \times 10}_{\text{k 10s}} = 10^k
\end{aligned}$$

10^k means there are k tens multiplied together - also written as a 1 followed by k zeros*. The above list explicitly shows the cases for $k = 2, 3$ and 4. Using the k like that is just a way to show that we can pick ANY whole number, i.e., there is no limit on how big k can be.

The notation of 10^k is handy and extends to the case when $k = 0$ and $k = 1$.

So 10^1 means* that there is only one ten multiplied together, or one "0" following the "1", in other words, just the number ten itself.

*k is called the "exponent" and you should read the symbol 10^k as "ten-raised-to-the-k^{th}-power" or "ten-to-the-k", so 10^2 is "ten raised to the second power" or 10^4 is "ten-to-the-fourth". You may also see 10^2 referred to as "ten squared", similarly 10^3 as "ten cubed" - but since we don't live in 4-dimensional hyperspace, we don't have a way of saying 10^4 that has geometric meaning.

*Don't forget to read 10^1 as "ten-to-the-one".

How about when $k = 0$? Examining the pattern of how the power k relates to how many zeros follow the "1" (eg, $10^1 = 10$, $10^2 = 100$, $10^3 = 1000$, etc.) then it must be the case that $10^0 = 1$, i.e., no zeros follow the "1", which is exactly right. Furthermore every number raised to the 0^{th} power is 1.[†]

Let's look at an example. Reading the number 92507 out according to our wordy technique above we can see that it's "nine lots of ten-thousand, plus two lots of a thousand, plus five lots of a hundred, plus zero lots of ten, plus seven units":

$$\begin{array}{rrcr} & 9 & \times & 10000 \\ + & 2 & \times & 1000 \\ + & 5 & \times & 100 \\ + & 0 & \times & 10 \\ + & 7 & \times & 1 \end{array} \quad = \quad \begin{array}{rr} & 90000 \\ + & 2000 \\ + & 500 \\ + & 00 \\ + & 7 \\ \hline = & 92507 \end{array}$$

Written[‡] in terms of powers-of-ten: $92507 = 9{\times}10^4 + 2{\times}10^3 + 5{\times}10^2 + 0{\times}10^1 + 7{\times}10^0$.

This way of breaking down the base-ten representation of a number into an algebraic expression can be done for EVERY string of decimal digits. It's the key to understanding what a string of decimal digits means.

Recalling that $10^0 = 1$ you might wonder why we bother to multiply $7{\times}10^0 = 7{\times}1 = 7$ since there is no actual effect when multiplying by one. Even though it's not necessary, including the 10^0 in the expression reveals a kind of mathematical symmetry. Each successive digit is multiplied by an ever decreasing power-of-ten, including the units-digit, which is just some number from 0 to 9 times a power-of-ten like any of the other digits.

Our example number 92507 only has five digits and it's biggest power-of-ten is 10^4, but there's no limit on how big a power-of-ten could be involved in our expression. Look at "a trillion and one", i.e.; 1,000,000,000,001 which can be expressed as:

$$1{\times}10^{12} + 0{\times}10^{11} + 0{\times}10^{10} + \cdots + 0{\times}10^2 + 0{\times}10^1 + 1{\times}10^0$$

Or pushing that limit to silly heights we can also describe this next ludicrous number. It's twenty-thousand-and-one digits long[§], a "7" followed by 9999 zeros, then a "3" followed by 9999 more zeros, then a "5", which means this:

$$7{\times}10^{20000} + 0{\times}10^{19999} + \cdots + 0{\times}10^{10001} + 3{\times}10^{10000} + 0{\times}10^{9999} + \cdots + 0{\times}10^1 + 5{\times}10^0$$

Clearly we can keep going as high as we like.

Let's use our understanding of counting in base-ten to build up to the "Basis Representation Theorem" introduced above.

We intuitively know that counting with base-ten covers all the positive integers. For example, the odometer in your car that keeps churning out new numbers for each mile you drive, starting from

[†]Proof: Since $a^{b+c} = a^b a^c$ consider when $c = 0$; that is, $a^b = a^{b+0} = a^b a^0$ so because of the uniqueness of the multiplicative-identity "1" (the uniqueness of 1 is a theorem and *not* an axiom) then a^0 *must* be 1 since it's behaving like a 1 in the expression $a^b = a^b a^0$.

[‡]Recall the mnemonic "bedmas" for the "Order of Operations" in evaluating an expression, which is no different from what we did in our table above the expression.

[§]A twenty-thousand-and-one digit long number is *ridiculously* large, consider that our estimate of the number of molecules in the entire universe would only need a base-ten number with the k set to somewhere between 78 and 82 to count them all.

zero when it rolls off the production line. If your odometer was long enough that it stretched off past the horizon on your left, there's no limit on how many miles you could count.

Our intuition is good - let's write it down in our theorem. We might say:

Base-Ten Representation Theorem (initial draft)

Every integer has a representation in base-ten.

Something else we know intuitively is that each number written in base-ten represents only ONE integer. It almost feels silly to spell it out, but if we were to count out 4 piles of 100-apples-each-pile, then 7 piles of 10-apples-each-pile, then count out 9 additional apples, *then* scoop them all into a big pile that we'd always get the exact same size big-pile-of-apples.

It goes the other way too. If we were handed the aforementioned big-pile-of-apples we could start counting out piles of 100. We'd try to make as many piles of 100 as we could, and we'd find that we'd have 4 piles of 100 before we couldn't make another such pile. Then we would start counting out piles of 10 with the remaining apples finding that we could only make seven such piles-of-ten, leaving nine single apples remaining, in other words, 479 apples! There is NO other way to divvy up this big-pile-of-apples if we follow this procedure. In other words, each integer is represented by only ONE base-ten number.

Let's strengthen our theorem based on the last two observations.

Base-Ten Representation Theorem (second draft)

Every integer has a *unique* representation in base-ten.

Let's not worry about negative integers for now, they're easy to represent once you have a way to represent positive integers, just slap a minus sign on the front to get the negatives. Also, moving forward it would be helpful to have a name for our positive integer so that we can refer to it directly - how about n for "number":

Base-Ten Representation Theorem (third draft)

Every *positive* integer n has a unique representation in base-ten.

At the moment it's not very helpful to have named n (the theorem as it stands doesn't say anything more about n so why did we bother naming it?) but as we flesh out the remaining details of the theorem we can refer to n which carries the important information that it could be ANY positive integer.

Earlier we looked at the number 92507 by adding up each digit times a power-of-ten*:

$$92507 = 9{\cdot}10^4 + 2{\cdot}10^3 + 5{\cdot}10^2 + 0{\cdot}10^1 + 7{\cdot}10^0$$

Every base-ten number implicitly describes an algebraic expression like this, so let's come up with a general expression of this form that can describe ANY positive integer n.

Let's replace one of the digits in our example number 92507 with d, how about the 5 like this $92d07$. What I mean becomes clear if I write it out:

$$n = 92d07 = 9{\cdot}10^4 + 2{\cdot}10^3 + d{\cdot}10^2 + 0{\cdot}10^1 + 7{\cdot}10^0$$

*It's time to replace our "×" symbol for multiplication, with "·" because "×" might get confused for an "x" in an expression, whereas "·" never will be. Eg. $x \times 2$ vs. $x \cdot 2$, additionally ending up with something that is more aesthetically pleasing. You may also see the "·" omitted entirely as in ab - which means $a \cdot b$ as you have seen in earlier footnotes.

So n is one of the following numbers: 92007, 92107, 92207, 92307, 92407, 92507, 92607, 92707, 92807 or 92907.

The digit d must be an integer between 0 and 9 inclusive which we can write as "$0 \leq d \leq 9$" however, I suggest that "$0 \leq d < 10$" is better*. It's logically equivalent to "$0 \leq d \leq 9$" but conveys more important information to the reader. Why even talk about nine when the theorem is about base TEN?

$$\begin{aligned} n = 9{\cdot}10^4 + 2{\cdot}10^3 + d{\cdot}10^2 + 0{\cdot}10^1 + 7{\cdot}10^0,&\text{ where} \\ d \text{ is an integer such that } 0 \leq d < 10& \end{aligned}$$

This statement for n only represents the integers 92007, 92107, ... or 92907, so let's come up with a statement for n that will allow us to generate ANY five-digit-number from 10000 the way up to 99999 (which is a complete list of all the five-digit-numbers).

In order to describe this general five-digit-number, we need five different 'd's, one for each of the five digits. In other words, we need to associate a different term d with each of the powers 10^4, 10^3, 10^2, 10^1 and 10^0.

Mathematics has a convention for coming up with a list of terms for situations just like this - we tack a subscript onto the name like so: d_2 which you read as "dee-two"†. d_2 is a term to represent a digit just like the d we used above. But now we can use that little subscript as a way to associate it to a specific power-of-ten. Naturally, we'll associate d_2 with 10^2 (ten squared) as follows:

$$\begin{aligned} n = 9{\cdot}10^4 + 2{\cdot}10^3 + d_2{\cdot}10^2 + 0{\cdot}10^1 + 7{\cdot}10^0,&\text{ where} \\ d_2 \text{ is an integer such that } 0 \leq d_2 < 10& \end{aligned}$$

If we define d_2 like this, then we know that when we refer to the digit d_2 that we are talking about the digit that is multiplied with 10^2.

Let our five-digit-number n use d_0, d_1, d_2, d_3 and d_4 for its digits. Then the general expression for n looks like this‡:

$$\begin{aligned} n = d_4{\cdot}10^4 + d_3{\cdot}10^3 + d_2{\cdot}10^2 + d_1{\cdot}10^1 + d_0{\cdot}10^0&\text{, where} \\ d_0 \text{ is an integer such that } 0 \leq d_0 < 10\text{, and}& \\ d_1 \text{ is an integer such that } 0 \leq d_1 < 10\text{, and}& \\ d_2 \text{ is an integer such that } 0 \leq d_2 < 10\text{, and}& \\ d_3 \text{ is an integer such that } 0 \leq d_3 < 10\text{, and}& \\ d_4 \text{ is an integer such that } 1 \leq d_4 < 10.& \end{aligned}$$

OK, hold on a minute - that's getting a little cumbersome. it's clunky and hard to read - plus did you notice how we slipped in that different range for d_4?

First, let's deal with the different range on that d_4. To make sure n is a legitimate five-digit-number we have to call out the exception that d_4 can NOT be zero - it has to be at least 1.

*Read $0 \leq d \leq 9$ as "zero is less-than-or-equal-to dee which is less-than-or-equal-to nine" and $0 \leq d < 10$ as "zero is less-than-or-equal-to dee which is (strictly) less-than ten".

†...yes like artoo-detoo, which perhaps George should have written "R_2D_2" and not "R2-D2"!

‡That expression looks like hard-core math, so let's take a moment to read it out loud, as a Math-Professor might do in a lecture. She might say: "n is equal to dee-four times ten-to-the-fourth, ... plus dee-three times ten-cubed, ... plus dee-two times ten-squared, ... plus dee-one times ten, ... plus dee-zero times one."

Why? Because if d_4 were zero then n would only be a four-digit-number, or perhaps a three-digit-number, or only two-digits etc.

Secondly, to clean up the presentation a common convention is to let another term like i, for perhaps "index", stand in for the subscript when you want to talk about all your 'd's at once:

> Let d_0, d_1, d_2, d_3 and d_4 be integers such that:
>
> $$n = d_4 \cdot 10^4 + d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$$
>
> where $0 \leq d_i < 10$ for all i in $\{0, 1, 2, 3, 4\}$ and $d_4 \neq 0$.

That's it! Those statements and the expression for n describe EVERY five-digit-number.

Now let's extend our five-digit-expression for n to an arbitrary number of digits. Consider the following progression:

expression for n	number-of-digits
$d_0 \cdot 10^0$	1
$d_1 \cdot 10^1 + d_0 \cdot 10^0$	2
$d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$	3
$d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$	4
$d_4 \cdot 10^4 + d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$	5
...	...
$d_k \cdot 10^k + \ldots + d_4 \cdot 10^4 + d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$	k+1

Using k like this let's us specify any number of digits we want. If we let $k = 0$ we get the first "single-digit" item on the list. $k = 4$ gives us our five-digit-number above, or we could let k be a twenty-thousand, which would allow us to specify an integer that has a twenty-thousand-and-one digits in it.

So there we have it, we found our expression for being able to express each positive integer, let's use it in the final draft of our base-ten-theorem.

Base-Ten Representation Theorem

> Let the two-digit-number "10" represent the integer ten.
>
> For every positive integer n there is a unique sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:
>
> $$n = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$$
>
> where $0 \leq d_i < 10$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.
>
> Definition: n is represented in base-ten by the string of digits $d_k d_{k-1} \cdots d_2 d_1 d_0$

Our newly added "Definition" introduces exactly what it means to write the number out in base-ten; that is, we toss out all the extraneous stuff from our expression and string all the digits one after another. Starting at the most-significant digit d_k on the left, down to the next digit to its right which is d_{k-1} (read as "dee-kay-minus-one"*) all the way down to the least-significant units-digit d_0 on the right.

*. . . and d_{k-1} is multiplied by "ten-to-the-power-of-(kay-minus-one)".

I also threw in the opening statement “Let the two-digit-number “10” represent the integer ten” since the theorem itself is defining what it even means to write out a multiple digit number, so until this theorem is established, “10” could mean anything.

Generalize the Theorem

Since the introduction of the EDVAC† computer, around 1950, there have been many orders of magnitude more calculations done in base-two (otherwise known as binary) by computers than have EVER been done by people in base-ten for the entirety of human history. This might even be true if we only count one-day’s worth of binary computer calculations - or perhaps even one-second’s worth of computer calculations across the whole world. Anyway, now-a-days the use of base-two eclipses that of base-ten.

Binary-computer logic gates (the building blocks of the modern computer) can only take one of two states, that is; “off” or “on”. We interpret these two states to represent these two numbers: 0 and 1. By doing so, in the same way that base-ten uses ten numbers 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9 for its digits, we can represent integers in base-two with just the digits 0 and 1. How is this possible?

Consider distant Planet-Nova on which the emergent intelligent species only have nine fingers on their hands. They have three hands with three fingers each - anyway, that’s why they use base-nine, so they only need the numbers 0, 1, 2, 3, 4, 5, 6, 7 and 8 for their digits‡. So like we Earthlings do for the integer ten, instead of making up a new symbol for nine, they use “10” to represent the integer nine - which for them means “One lot of nine, plus zero units”.

Similarly on Planet-Ocho, since they only have eight fingers, then they use base-eight and only use numbers 0, 1, 2, 3, 4, 5, 6 and 7 for their digits. For them, “10” means “One lot of eight, plus zero units”.

On and on past Planet-Gary-Seven (they have only seven fingers), and Planet-Hex (six fingers), Planet-Penta (five fingers), etc...

Finally, we come upon Planet-Claire (well someone has to come from Planet-Claire, I know she came from there), where they only have two fingers so they only use the digits 0 and 1 and base-two, so for them, “10” means “one lot of two and zero units”. So on Planet-Claire “10” means two. Recall above how we arrived at our 100 in base-ten, being “ten lots of ten, plus zero units” - similarly on Planet-Claire “100” in base-two for them means “Two lots of two plus zero units” in other words, four! What is “11” in base-two? Using our technique to describe the digits we see that it’s “One lot of two, plus one unit”, in other words, three.

†You might be thinking, don’t you mean ENIAC which was earlier? Actually no - the ENIAC used base-ten accumulators, not binary!

‡Digit is another word for finger! Of course,, that’s where the math term got its start.

Here's how they count on Planet-Claire using base-two:

base-two	base-ten	base-two	base-ten
0	0	(. . . cont)	
1	1	1101	13
10	2	1110	14
11	3	1111	15
100	4	10000	16
101	5	10001	17
110	6	. . .	
111	7	11111	31
1000	8	100000	32
1001	9	. . .	
1010	10	1000000	64
1011	11	10000000	128
1100	12 (cont. . .)	100000000	256

Note something interesting in the list above - the powers of two, written in base-two, resemble our powers of 10 in base-ten! That is:

$$\begin{array}{rcl} 1 = 2^0 = 1, & \qquad & 32 = 2^5 = 100000_{\text{(base-2)}}, \\ 2 = 2^1 = 10_{\text{(base-2)}}, & & 64 = 2^6 = 1000000_{\text{(base-2)}}, \\ 4 = 2^2 = 100_{\text{(base-2)}}, & & 128 = 2^7 = 10000000_{\text{(base-2)}}, \\ 8 = 2^3 = 1000_{\text{(base-2)}}, & & 256 = 2^8 = 100000000_{\text{(base-2)}}, \\ 16 = 2^4 = 10000_{\text{(base-2)}}, & & \ldots \end{array}$$

Let's look at the binary number 11010 for example. Using our wordy technique to describe the number we can see that it's "One lot of sixteen, plus one lot of eight, plus zero lots of four, plus one lot of two, plus zero units":

$$\begin{array}{ccccr} & 1 & \times & 10000 \\ + & 1 & \times & 1000 \\ + & 0 & \times & 100 \\ + & 1 & \times & 10 \\ + & 0 & \times & 1 \end{array} \quad = \quad \begin{array}{crl} & 10000 & (16) \\ + & 1000 & (8) \\ + & 000 & \\ + & 10 & (2) \\ + & 0 & \\ \hline = & 11010 & (26) \end{array}$$

Written in terms of powers of two: $11010_{\text{(base-2)}} = 26 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$.

Does that expression look familiar? It has exactly the same form as the expression for our five-digit base-ten number 92507. All the reasoning we used to come up with the statement of the "Base-Ten Representation Theorem" can be used again, but swapping powers-of-two for powers-of-ten, and limiting the values for the digits to be zero or one. Following our line of reasoning this is what the Planet-Claire mathematicians would have come up with. . .

Base-Two Representation Theorem

For every positive integer n there is a unique sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k 2^k + d_{k-1} 2^{k-1} + \cdots + d_2 2^2 + d_1 2^1 + d_0 2^0,$$

where $0 \leq d_i < 2$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

Definition: n is represented in base-two by the string of binary-digits $(d_k d_{k-1} \cdots d_2 d_1 d_0)_2$

Our new Base-Two Representation Theorem introduced some helpful new notation in the "Definition". How do you know what I'm talking about if I just write "1000"? Do I mean 10^3 or 2^3? If there is any possibility for confusion we write the number like this $(1000)_{10}$ for the base-ten version meaning one-thousand and $(1000)_2$ for the binary version meaning eight. That's what the "Definition" is spelling out with the "$(\ldots)_2$" notation.

As is hinted by the habits of our various alien friends above it seems that we can use ANY integer greater than or equal to 2 as a base. In fact computer graphics artists are known to stumble upon numbers written in hexadecimal (usually relating to specifying a color-channel), which is base-sixteen.

Base-sixteen introduces some new single-character symbols to the usual numbers 0, 1, 2, thru 9, to represent the numbers 10, 11, 12, 13, 14 and 15. Base-sixteen adds the digits A, B, C, D, E and F where $A_{16}=(10)_{10}$, $B_{16}=(11)_{10}$, $C_{16}=(12)_{10}$, $D_{16}=(13)_{10}$, $E_{16}=(14)_{10}$, $F_{16}=(15)_{10}$. For example, $(97A3F2)_{16}$ is a four-digit-number in base-sixteen (which means $(9{,}937{,}906)_{10}$ in base-ten.)

Note that if we omit the parentheses and subscript from a number, it means we're talking about it in base-ten; our "default" base. Case in point: the subscripts that we use to denote the base (like the "16" in $(97A3F2)_{16}$) are written in base-ten.

We could go ahead and prove our "Base-Ten" and "Base-Two" theorems above, but what about proving the "Base-Nine" version of the theorem for the aliens on Planet-Nova, or the "Base-Eight" version for the inhabitants of Planet-Ocho?

To cover all bases (pun intended) let's restate our theorem for the general case, call it "base-b", where b is some number greater than or equal to two. If we can prove that theorem, then we'll automatically get all the cases of specific bases for free.

Here is our hero-theorem again, but this time, armed with your new mathematical vocabulary and understanding I expect that this theorem will make much more sense to you.

Basis Representation Theorem

Let b be a positive integer greater than 1.

For every positive integer n there is a unique sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0,$$

where $0 \leq d_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

Definition: n is represented in base-b by the string of base-b-digits $(d_k d_{k-1} \cdots d_2 d_1 d_0)_b$

So to get the "Base-Ten Representation Theorem" let b equal ten. To get the "Base-Two Representation Theorem" let $b = 2$; or the "Base-Nine Representation Theorem" let $b = 9$; etc.

Recall how we defined $(\mathrm{A})_{16} = 10$ and $(\mathrm{F})_{16} = 15$ as base-sixteen digits, then:

$$(97\mathrm{A}3\mathrm{F}2)_{16} = 9 \cdot 16^5 + 7 \cdot 16^4 + 10 \cdot 16^3 + 3 \cdot 16^2 + 15 \cdot 16^1 + 2 \cdot 16^0 = 9,937,906$$

. . . which gives you an idea of how you can convert from an alternate base into base-ten.

Before we dive into proving the theorem please try some exercises for fun. Mathematics is more enjoyable if you get your hands dirty, it's not just a spectator sport. You should be able to do these exercises but if you get stuck (or to check your work) the answers are supplied below - but please don't peek until you try the questions yourself.

If you feel bewildered when facing the exercises, know that you are in good company - this is a common feeling among mathematicians, you'll get used to it. But like any exercise in a workout if you push on through you will get stronger. (Hint: A pocket calculator will be helpful.)

Exercises

1. What are the following numbers expressed in base-ten?
   i) $(110101)_2$
   ii) $(\mathrm{A}053\mathrm{D})_{16}$
   iii) $(1017)_{23}$
2. What are the following base-ten numbers expressed in an alternate base?
   i) 33 expressed in base-two?
   ii) 127 expressed in base-two? (Hint: $127 = (128 - 1)$)
   iii) 8079 expressed in base-sixteen?

   Hint: For a moment, pretend that we don't use base-ten to write out our numbers, instead picture a pile of apples. Can you picture 7654 apples? Yes? Good let's use 7654 as our example.

   Let's divide 7654 by 10 so we get the following:

   $$7654 = 765 \cdot 10 + 4$$

   Notice the remainder 4 is the least-significant-digit of our integer 7654 (i.e. the d_0 digit in the theorem).

   How do we get the next digit, i.e. the d_1 digit that corresponds to the 10^1 term? Well, its kind of cheating, but since we happen to be looking at that last expression written in base-ten we can see it sitting right there in at the end of the quotient "765". So, let's use the same technique and divide 765 by 10:

   $$765 = 76 \cdot 10 + 5$$

   So the remainder is 5 our d_1 digit. Let's keep going, this time dividing the previous quotient 76 by 10.. . .

   $$76 = 7 \cdot 10 + 6$$

and finally,

$$7 = 0 \cdot 10 + 7$$

So, our series of remainders happens to be the digits of the number in base-ten. Specifically $d_3 = 7$, $d_2 = 6$, $d_1 = 5$ and $d_0 = 4$.

Try doing that for 8079, but use 16 instead of 10 as the divisor.

iv) Let $\mathrm{A}_{23} = 10, \mathrm{B}_{23} = 11, \mathrm{C}_{23} = 12, \mathrm{D}_{23} = 13, \mathrm{E}_{23} = 14, \mathrm{F}_{23} = 15, \mathrm{G}_{23} = 16,$ $\mathrm{H}_{23} = 17, \mathrm{I}_{23} = 18, \mathrm{J}_{23} = 19, \mathrm{K}_{23} = 20, \mathrm{L}_{23} = 21$ and $\mathrm{M}_{23} = 22$, then what is 185190 expressed in base-twenty-three?

v) 291480 expressed in base-twenty-three?

Answers

1. What are the following numbers expressed in base-ten?
   i) $(110101)_2 = 53$
   ii) $(\mathrm{A053D})_{16} = 656701$
   iii) $(1017)_{23} = 12197$
2. What are the following base-ten numbers expressed in an alternate base?
   i) $33 = (100001)_2$
   ii) $127 = (1111111)_2$
   iii) $8079 = (\mathrm{1F8F})_{16}$
   iv) $185190 = (\mathrm{F51H})_{23}$
   v) $291480 = (\mathrm{10M01})_{23}$

Introduction to Proofs

There are several ways to approach proving The Basis Representation Theorem.

The mathematician George E. Andrews (in his book "Number Theory") has an interesting proof. He asks us to imagine a that we have at our disposal a function that when fed a positive integer n, returns to us a count of the number of base-b representations of n. Then with some fairly straightforward reasoning he shows that this counting-function MUST produce a count of "1" for every n, both establishing the uniqueness and the existence in one fell swoop.

We could also prove The Basis Representation Theorem by dividing our integer n by b, then dividing that result by b again, then again, and again, etc. We'd end up with a finite-length series of remainders which are the base-b-digits of n. This is an interesting approach to the proof in that it also gives us a technique to construct a base-b representation of each integer. If we were to go down this road we would try to generalize how we solved exercise number 2-iii above.

However, we're going to follow a much more straightforward approach. We'll use the principle of mathematical induction directly on n to prove that a base-b representation of each positive integer exists. Then we'll use a different approach to prove that each such representation is unique.

The Principle of Mathematical Induction

Recall that when we talk about positive integers in mathematics, we're talking about the set of numbers that represent successively larger piles of apples starting with a pile containing only one apple.

So we start with "🍎" to get our very first smallest pile of apples. Then add another apple to get a pile of "🍎🍎", then "🍎🍎🍎", then "🍎🍎🍎🍎" then some big pile of "🍎🍎🍎🍎🍎...🍎🍎🍎" after we've been adding apples for a while. Each successively bigger pile of apples corresponds with each successive positive integer. We keep adding one more to get the next integer, we keep adding one more, over and over forever to get them all.

This idea of being able to step one after the other, beginning at 1 and going forever is embodied within the principle of mathematical induction and is a basic property of the positive integers. This principle is more than just a way to generate the set of integers, it's also a way of thinking about properties of the integers.

Suppose that $P(n)$ means that the property P holds for the number n; where n is a positive integer. Then the principle of mathematical induction states that $P(n)$ is true for ALL positive integers n provided that[*]:

i) $P(1)$ is true

ii) Whenever $P(k)$ is true, $P(k+1)$ is true.

Why would these two conditions show that $P(n)$ is true for all positive integers? Note that condition ii) only asserts the truth of $P(k+1)$ under the assumption that $P(k)$ is true. However, if we also know that $P(1)$ is true then condition ii) implies that $P(2)$ is true, which again implies

*This wording of the definition of "The Principle of Mathematical Induction" is essentially borrowed from "Calculus" by Michael Spivak - a fabulous introductory textbook on Analysis.

that $P(3)$ is true, which in turn leads to the truth of $P(4)$, etc., over and over for all positive integers.

Some people picture an infinite row of dominoes. Having condition i) (called the “base case”) is like being able to knock over the first domino. Then knowing that condition ii) is also true (called the “induction step”) is like the fact that any one domino has the ability to knock over the next. Once you’ve knocked over the first domino, they all fall.

Let’s look at a simple example: Perhaps you’ve heard the story of young Carl Friedrich Gauss as a boy in the 1780s who was assigned (along with all his classmates) the tedious task of summing the first 100 integers - presumably to keep them quiet and busy while the teacher corrected some papers. Anyway, young Gauss immediately produced the answer, 5050, before most of the boys had summed the first couple of numbers.

It wasn’t young Gauss’s extraordinary computational speed which allowed him to perform this dazzling task, but he had the deeper insight that instead of adding 1 plus 2, then adding 3, then 4, etc. he saw that if you paired 1 with 100, and 2 with 99, and 3 with 98, etc., that each of those pairs added up to 101, furthermore he knew he’d have 50 such pairs, meaning he could state the result in a heartbeat - tada - “5050”! Gauss is widely regarded as being one of the greatest mathematicians who have ever lived - the young eight-year-old was just getting started.

Anyway, to generalize young Gauss’s insight we can write the expression like this:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

So let’s prove this relationship using the principle of mathematical induction.

Let $n = 1$ for the “base case”, then

$$\frac{1(1+1)}{2} = \frac{2}{2} = 1$$

Which is the trivial sum* of the first positive integer 1.

Now let’s assume the relationship is true for n, and prove that it must also be true for $n+1$ for our “induction step”:

$$\begin{aligned}
& (1+2+3+\ldots+n)+(n+1) && \text{(Add together 1 through } n+1.\text{)} \\
&= \frac{n(n+1)}{2} + (n+1) && \text{(Substitute induction assumption for 1 through } n.\text{)} \\
&= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} && \text{(Common denominator of 2.)} \\
&= \frac{n^2+n+2n+2}{2} && \text{(Multiply out numerator.)} \\
&= \frac{n^2+3n+2}{2} && \text{(Add like terms.)} \\
&= \frac{(n+1)(n+2)}{2} && \text{(Factor numerator.)} \\
&= \frac{(n+1)((n+1)+1)}{2} && \text{(Rewrite in terms of } (n+1).\text{)}
\end{aligned}$$

*The word “sum” here is used in the context of the expression we are trying to prove. In this case we are summing only one item thus it’s “trivial”.

Which proves young Gauss's expression is true for the positive integer $n+1$ whenever it's true for n (to see this, compare our new expression for adding the first $(n+1)$ integers to the expression for n that we're trying to prove) - then by the principle of mathematical induction, the expression is true for all positive integers. QED*

Extra Exercise: Geometric Series Theorem

If b, n are non-negative integers and $b \neq 1$ then prove,

$$1 + b + b^2 + \cdots + b^{n-1} = \frac{b^n - 1}{b - 1}$$

Hint: use induction on n, the base case being $n = 1$. Before you turn the page, try proving this, you can do it!

* "QED" - is often used at the conclusion of a proof to state that it's done - it's an acronym for the Latin phrase "quod erat demonstrandum" which means "that which was to be demonstrated". In other words, we've proven what we set out to prove.

Proof for Extra Exercise: Geometric Series Theorem

Base case: $n = 1$

$$\frac{b^1 - 1}{b - 1} = \frac{b - 1}{b - 1} = 1 = b^0 = b^{1-1}$$

Induction step: Assume the following

$$1 + b + b^2 + \cdots + b^{n-1} = \frac{b^n - 1}{b - 1}$$

Then,

$$\begin{aligned}
& (1 + b + b^2 + \cdots + b^{n-1}) + b^n && \text{(Add } n+1 \text{ terms of series together.)} \\
&= \frac{b^n - 1}{b - 1} + b^n && \text{(Substitute induction assumption for first } n \text{ terms.)} \\
&= \frac{b^n - 1}{b - 1} + \frac{b^n(b - 1)}{b - 1} && \text{(Common denominator of } b-1\text{.)} \\
&= \frac{b^n - 1 + b^{n+1} - b^n}{b - 1} && \text{(Multiply out numerator.)} \\
&= \frac{b^{n+1} + b^n - b^n - 1}{b - 1} && \text{(Reorder terms (Associativity).)} \\
&= \frac{b^{n+1} - 1}{b - 1} && \text{(Adding then subtracting } b^n \text{ is zero.)}
\end{aligned}$$

QED

Idea behind Induction Proof for the Basis-Reprn-Thm

Using the principle of mathematical induction to prove that a base-b number exists for all the positive integers is pretty simple. The crux of the approach is to show that if n can be expressed in base-b, then it necessarily follows that $n + 1$ can also be represented in base-b.

Let's pretend we just bought a brand-new car with one of those physical odometers that spin little wheels to show the number of miles driven. According to the brochure our new car has a magic-odometer. We notice as we pull out of the dealership parking lot that the odometer is only one digit wide and that one-and-only-digit displays a "1", I guess the factory was only one mile away.

As we get close to the end of our drive home we see we've clocked 9 miles. Naturally we're a little curious about how it's going to count to ten since the odometer apparently only has one digit. While pondering this curiosity we see the 9 starting to roll over back to 0, and a second digit to it's left magically materializes! It rolls to a 1 as the 9 settles back to 0. Apparently this magic-odometer only adds new digits to the left as it needs them. The magic-odometer should be able to display ANY number of miles, no matter how large.

Our proof is going to take care of the three cases that happen with the magic-odometer. Imagine that we've already driven some arbitrarily large number of miles, and we're watching the odometer roll over to the next mile. We have the following cases:

i) The units-digit is less than 9, so driving one more mile only increments the units-digit, not affecting any of the other digits.

   Example: We've driven 782995 miles so far, so the next mile driven is $782995 + 1 = 782996$.

   So that units-digit turned from a "5" to a "6", all the rest of the digits remaining unchanged, so the new number is a legitimate base-ten number.

ii) The units-digit, and perhaps a few directly to the left of it, are all 9's, so driving one more mile will spin all those 9's to 0, at the same time incrementing the rightmost-digit *that isn't a* 9 by one.

   Example: We've driven 782999 miles so far, so the next mile driven is:

$$\begin{aligned}782999 + 1 &= 780000 + 2000 + 999 + 1\\ &= 780000 + 2000 + (1000 - 1) + 1\\ &= 780000 + 2000 + 1000 + (-1 + 1)\\ &= 780000 + 3000 + 0\\ &= 783000\end{aligned}$$

   That looks overly complicated, but I broke it down like that to demonstrate the idea behind the algebra that's used in the actual proof.

   Anyway, it's clear that the rightmost-digit that-isn't-a-9, in our case the 2, got changed to a 3 and all the 9's got changed to 0's, while the rest of the digits remained unchanged leaving us with a legitimate base-ten number.

iii) ALL the digits from the units-digit up to the highest-digit are 9's, so driving one more mile engages the magic-odometer feature, materializing a new leftmost-digit. The newly materialized digit turns to a 1 and all the 9's spin back to 0. In this case the number of digits on the odometer will have been extended by one.

   Example: We've driven 999999 miles so far, so the next mile driven is:

$$\begin{aligned}999999 + 1 &= (1000000 - 1) + 1\\ &= 1000000 + (-1 + 1)\\ &= 1000000 + 0\\ &= 1000000\end{aligned}$$

   This uses the same kind of algebraic manipulation as the previous case, but this time our number grew from a six-digit-number to a seven-digit-number. Yup, we just drove a million miles which is definitely a legitimate base-ten number.

Without further adieu, let's get to the actual proof!

Existence Proof of the Basis Representation Theorem

Let b be a positive integer greater than 1.

Using induction we will show that for every positive integer n there is a sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0,$$

where $0 \leq d_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

We will henceforth refer to the above expression for n as the "base-b-representation" for n.

Base case:

Consider when $n = 1$.

Let $d_0 = 1$ be the only integer in the sequence. Then,

$$d_0 b^0 = 1 \cdot b^0 = 1 \cdot 1 = 1 = n$$

Since $d_0 < b$ and $d_0 \neq 0$ (note: $k = 0$) then this shows that a base-b-representation exists for the integer 1.

Induction Step:

Let n be a positive integer, and assume that there is a sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0,$$

where $0 \leq d_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

We will prove that $n + 1$ also has a base-b-representation by looking at two cases.

Case 1) $d_0 < (b - 1)$

This case examines when the least-significant-digit of n is *strictly-less-than* the largest value it can take in base-b. (For example, in base-two $d_0 = 0$; In base-five $d_0 \leq 3$; In base-ten $d_0 \leq 8$.)*

$$\begin{aligned}
& & n &= d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0 && \text{(Induction Assumption)} \\
&\Leftrightarrow & n + 1 &= d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0 + 1 && \text{(Add 1 to both sides)} \\
& & &= d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0 + b^0 && \text{(Restate 1 as } b^0\text{)} \\
& & &= d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + (d_0 + 1) b^0 && \text{(Axiom of Distribution)}
\end{aligned}$$

The expression for $n + 1$ uses the same sequence of integers $d_k, d_{k-1}, \ldots, d_2, d_1$ as n, with only change being that the integer d_0 was altered to $(d_0{+}1)$, but since:

$$\begin{aligned}
& & d_0 &< (b - 1) && \text{(Case 1 Assumption)} \\
&\Leftrightarrow & d_0 + 1 &< (b - 1) + 1 && \text{(Add 1 to both sides)} \\
&\Leftrightarrow & d_0 + 1 &< b
\end{aligned}$$

Therefore, given the conditions of "Case 1", $n + 1$ has a base-b-representation whenever n does.

*Please read the following bidirectional arrow symbol $\Leftrightarrow$ as "if and only if" - it's like a logical "equals" sign

Case 2) $d_0 = (b-1)$

Now we'll look at the case when the least-significant-digit of n is *exactly-equal-to* the largest value it can take in base-b. (For example, in base-two $d_0 = 1$; in base-five $d_0 = 4$; in base-ten $d_0 = 9$.)

We're going to split this case into two cases.

a) *All* the digits of n are equal-to $b-1$ (eg. 999999 in base-ten).

b) $d_0 = (b-1)$ but *at least one other* digit is not-equal-to $(b-1)$ (eg. 782999 in base-ten).

Case 2a) ALL of the digits of n are equal to $(b-1)$.

So n can be expressed like this:

$$n = (b-1)b^k + \ldots + (b-1)b^2 + (b-1)b^1 + (b-1)b^0 \quad \text{(Induction Assumption)}$$

Recall in the "Extra Exercise: Geometric Series Theorem" we showed that:

$$1 + b + b^2 + \ldots + b^k = \frac{b^{k+1}-1}{b-1}$$

We can use this theorem to show that $n+1 = b^{k+1}$ as follows...

$$\begin{aligned}
& b^k + \ldots + b^2 + b + 1 = \frac{b^{k+1}-1}{b-1} && \text{(Reorder terms of G.S.Thm.)} \\
\Leftrightarrow\quad & b^k + \ldots + b^2 + b^1 + b^0 = \frac{b^{k+1}-1}{b-1} && \text{(Rewrite with } b^1, b^0\text{)} \\
\Leftrightarrow\quad & (b-1)(b^k + \ldots + b^2 + b^1 + b^0) = b^{k+1} - 1 && \text{(Mult both side by } (b-1)\text{)} \\
\Leftrightarrow\quad & (b-1)b^k + \ldots + (b-1)b^1 + (b-1)b^0 = b^{k+1} - 1 && \text{(Distribution of } (b-1)\text{)} \\
\Leftrightarrow\quad & n = b^{k+1} - 1 && \text{(Substitute } n \text{ for expression)} \\
\Leftrightarrow\quad & n + 1 = b^{k+1} && \text{(Add 1 to both sides)}
\end{aligned}$$

Let's rewrite $n+1$:

$$n + 1 = 1 \cdot b^{k+1} + 0 \cdot b^k + \ldots + 0 \cdot b^2 + 0 \cdot b^1 + 0 \cdot b^0,$$

Therefore, given the conditions of "case 2a", $n+1$ has a valid base-b-representation whenever n does. We note that the number of integers in the sequence associated with $n+1$ is one longer than for n. i.e., $n+1$ is one digit longer that n.

Case 2b) $d_0 = (b-1)$ but at least one other digit is not equal to $(b-1)$

Let j be the lowest power-of-b such that $d_j < (b-1)$, i.e.; we can write n as follows:

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_j b^j + (b-1)b^{j-1} + \cdots + (b-1)b^1 + (b-1)b^0$$

Similar to how we used the "Geometric Series Theorem" above, we can simplify the expression for n as follows:

$$\begin{aligned}
& n = d_k b^k + \cdots + d_j b^j + \big((b-1)b^{j-1} + \cdots + (b-1)b^1 + (b-1)b^0\big) && \\
\Leftrightarrow\quad & n = d_k b^k + \cdots + d_j b^j + (b^j - 1) && \text{(Geom. Series Thm.)} \\
\Leftrightarrow\quad & n + 1 = d_k b^k + \cdots + d_j b^j + b^j && \text{(Add 1 to both sides)} \\
\Leftrightarrow\quad & n + 1 = d_k b^k + \cdots + (d_j + 1) b^j && \text{(Distr Axiom)}
\end{aligned}$$

Rewriting the expression for n in explicit terms:

$$n + 1 = d_k b^k + \cdots + d_{j+1} b^{j+1} + (d_j + 1)b^j + 0{\cdot}b^{j-1} + \ldots + 0{\cdot}b^1 + 0{\cdot}b^0$$

We can see that the expression for $n + 1$ uses the same sequence of integers $d_k, \ldots, d_{j+1}$ as n. The integer d_j was altered to $(d_j{+}1)$, which is a valid digit since:

$$\begin{aligned} & d_j < (b-1) && \text{(Previous assumption)} \\ \Leftrightarrow\quad & d_j + 1 < (b-1) + 1 && \text{(Add 1 to both sides)} \\ \Leftrightarrow\quad & d_j + 1 < b && \end{aligned}$$

Furthermore the remaining sequence of integers $d_{j-1} = \ldots = d_2 = d_1 = d_0 = 0$.

Therefore, given the conditions of "case 2b", $n{+}1$ has a valid base-b-representation whenever n does.

Taking "Case 1" and "Case 2" together proves that $n{+}1$ always has a base-b-representation whenever n does. Having also established the base-case, therefore by the principle of mathematical induction all positive integers have a base-b-representation.

QED

Idea behind Uniqueness Proof for the Basis-Reprn-Thm

Even though we can use induction to prove the existence of base-b numbers for every integer, let's think about why it doesn't prove the "uniqueness" aspect of the theorem. Imagine a magic-box that also makes base-b representations for each integer. In other words, if the odometer is the principle-of-mathematical-induction then the magic-box is some different mechanism working in a different way. Why not? We weren't careful to show that induction is the ONLY way to generate a base-b representation for each number. (It isn't.)

So we need to prove that if such a magic-box exists then it MUST produce the same results as our odometer.

The easiest way to prove this is to assume that there is a magic-box that DOES NOT produce the same representation as our odometer, then we show that this assumption leads to an irreconcilable contradiction. So either our assumption is wrong or the axioms are. Since we're VERY confident in the axioms being correct we can only conclude that our assumption must be wrong - meaning that there is only *one* way to make a base-b representation for each integer.

In order to proceed, we need to make use of a well-established theorem called the "Euclidean Division Theorem". It sounds onerous, but don't worry, you learned it in the third grade when you learned how to divide. It simply states the following. . .

Euclidean Division Theorem

For all integers a and b such that $b > 0$, there exist *unique* integers q and r such that[*]:

$$a = qb + r \text{ such that } 0 \leq r < b$$

Definition: In the above equation:

a is the *dividend*	("the number being divided")
b is the *divisor*	("the number doing the dividing")
q is the *quotient*	("the result of the division")
r is the *remainder*	("the leftover")

This is how you first learned to divide. For example, if someone asks you "What is nineteen divided by three?", you'd answer "six with one remaining". Here 19 is the *dividend*, 3 is the *divisor*, 6 is the *quotient* and 1 is the *remainder*. Written in the form of the theorem:

$$19 = 6 \cdot 3 + 1$$

Often proofs make use of little mini-theorems of their own. Creating these mini-theorems is a way to simplify a step in the main proof by establishing a useful intermediary result. It makes reading the main proof easier to follow by not having us get sidetracked with the technicalities of a step we want to make. These mini-theorems are called "Lemmas". We're going to make a lemma to help with proving the uniqueness part of the Basis Representation Theorem. But first we're going to make use of the Euclidean Division Theorem to prove our lemma.

Lemma

Let b, q and r be integers such that $b > 0$ and $0 \leq r < b$, then:

$$0 = qb + r \qquad \text{if and only if} \qquad q = 0 \text{ and } r = 0.$$

Proof of Lemma

Let b, q and r be integers such that $b > 0$ and $0 \leq r < b$.

If $q = 0$ and $r = 0$, then
$qb + r = 0 \cdot b + 0 = 0$

[*]Aside: Actually the theorem is stronger than we have stated here. Specifically, it only requires that $b \neq 0$, however, to keep the remainder positive, the restriction on r would have to be stated like this $0 \leq r < |b|$ to deal with the possibility that b might be negative.

Also if $0 = qb + r$, then clearly $q = 0$ and $r = 0$ satisfy the equation, but by the constraints placed on the values for b and r, then the Euclidean Division Theorem tells us that q and r are unique, therefore $q = 0$ and $r = 0$ is the only solution to this equation.

QED

Uniqueness Proof of the Basis Representation Theorem

Let b be a positive integer greater than 1.

By the "Existence Proof of the Basis Representation Theorem" we know that for every positive integer n there is a sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0$, where
$0 \le d_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \ne 0$.

Assume this expression for n is not unique and that there also exists a different sequence of integers $c_0, c_1, c_2, \ldots, c_k$ such that:

$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_2 b^2 + c_1 b^1 + c_0 b^0$, where
where $0 \le c_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $c_k \ne 0$.

Let's further suppose that j is the lowest power such that the integers $d_j \ne c_j$ and without any loss of generality let's assume that $d_j > c_j$. Since both expressions are equal to n then:

$$c_k b^k + \cdots + c_2 b^2 + c_1 b^1 + c_0 b^0 = d_k b^k + \cdots + d_2 b^2 + d_1 b^1 + d_0 b,$$

if and only if,

$$\begin{array}{rll}
& 0 = (d_k - c_k) b^k + \cdots + (d_j - c_j) b^j & \text{(Subtract left-side from both-sides)} \\
\Leftrightarrow & \dfrac{0}{b^j} = \dfrac{(d_k - c_k) b^k + \cdots + (d_j - c_j) b^j}{b^j} & \text{(Divide by } b^j\text{, since } b > 0) \\
\Leftrightarrow & 0 = (d_k - c_k) b^{k-j} + \cdots + (d_{j+1} - c_{j+1}) b + (d_j - c_j) & \text{(Divide each term in numerator by } b^j) \\
\Leftrightarrow & 0 = \big((d_k - c_k) b^{k-j-1} + \cdots + (d_{j+1} - c_{j+1})\big) b + (d_j - c_j) & \text{(Factor out common } b)
\end{array}$$

Let $q = \big((d_k - c_k) b^{k-j-1} + \cdots + (d_{j+1} - c_{j+1})\big)$, then

$$0 = qb + (d_j - c_j)$$

Since $0 \le (d_j - c_j) < b$ and $b > 0$ then by our lemma we know that $q = 0$ and $d_j - c_j = 0$.

But $d_j - c_j = 0$ if and only if $d_j = c_j$ contradicting our assumption that $d_j \ne c_j$. This implies that the initial assumption that "n is not unique" is *false*, in other words:

The base-b representation of n is unique.
QED

Since we have proven that a base-b-representation exists for ALL the positive integers *and* that this representation is unique, then we have proven the Basis Representation Theorem.

Epilogue

I wrote this paper with a technically savvy audience in mind, namely the many talented visual effects artists that I've worked with over the years who mainly graduated from Art College. Since Art College doesn't usually place an emphasis on higher level mathematics these younger artists may not have been exposed to it - and yet they use tools on a daily basis that are essentially high-level math applications.

If that describes you, then my hope with the paper is that by taking a familiar and simple subject, like counting, and applying rigorous mathematical reasoning, that you will become familiar with its "language" and get a taste for the sharpness of the thought process. Most importantly I hope you found some amusement in and among the mathematical tidbits sprinkled here and there.

I know you are very sensitive to beauty, after all, you are an artist so my hope is to open one more avenue to you to appreciate the beauty that mathematics has to offer, which rivals and perhaps eclipses any musical composition or painting or sculpture.

I don't claim that this particular paper contains such beauty (well, the Geometric Series Theorem is pretty elegant and nifty) but being comfortable with the language of mathematics will at least allow you to get to some of those marvelous results. I suggest Googling "Taylor Series" and "Maclaurin Series" which now that you are a little more comfortable with reading "mathy" statements, it might begin to make sense reading a wiki page.

Following that thread will take you to an amazing place, one the connects the trigonometric functions like sine and cosine with the natural logarithm in totally unexpected ways. Those mathematical discoveries point to some deep simple structure that underlies our world that without mathematics you wouldn't get to glimpse. It is truly awe-inspiring to experience for the first time - enjoy!